Roll No.											

PRESIDENCY UNIVERSITY

BENGALURU

End - Term Examinations – December 2025

Date: 10- 12- 2025 **Time:** 1.00pm to 04.00pm

School: SOCSE	**Program:** B. Tech Cyber Security	
Course Code: CCS2500	**Course Name:** Cyber Forensics	
Semester: V	**Max Marks**: 100	**Weightage**: 50%

CO - Levels	**CO1**	**CO2**	**CO3**	**CO4**	**CO5**
Marks	**26**	**24**	**24**	**26**	**-**

Instructions:

(i) Read all questions carefully and answer accordingly.
(ii) Do not write anything on the question paper other than roll number.

Part A

Answer ALL the Questions. Each question carries 2marks. **10Q x 2M=20M**

1.	Define 'Digital Evidence'.	**2 Marks**	**L1**	**CO1**
2.	What does 'Modus Operandi' mean in the context of a computer crime?	**2 Marks**	**L1**	**CO1**
3.	Differentiate between 'Motive' and 'Intent' in a digital investigation.	**2 Marks**	**L2**	**CO1**
4.	What is the purpose of a 'file signature'?	**2 Marks**	**L1**	**CO2**
5.	Convert the hexadecimal number *2F* to its decimal equivalent.	**2 Marks**	**L2**	**CO2**
6.	List two benefits of following a professional forensic methodology.	**2 Marks**	**L1**	**CO3**
7.	How does 'Identity Theft' differ from 'Identity Fraud'?	**2 Marks**	**L2**	**CO4**
8.	Define 'Chain of Custody'.	**2 Marks**	**L1**	**CO4**
9.	Why is volatile evidence collected first in a live system seizure?	**2 Marks**	**L2**	**CO4**
10.	Predict a potential consequence of failing to properly document the chain of custody for a digital evidence item.	**2 Marks**	**L3**	**CO4**

Part B

Answer the Questions. **Total Marks 80M**

11.	**a.**	List and explain the key stages of the digital investigative process.	**10 Marks**	**L2**	**CO1**
	b.	Summarize the importance of 'Investigative Reconstruction' in solving a computer crime.	**5 Marks**	**L1**	**CO1**
	c.	Identify the primary challenge of presenting digital evidence in a courtroom.	**5 Marks**	**L1**	**CO1**
Or					
12.	**a.**	Enumerate the historical milestones that shaped the field of computer crime investigation.	**10 Marks**	**L2**	**CO1**
	b.	Outline the role of technology in the evolution of criminal 'Modus Operandi'.	**5 Marks**	**L1**	**CO1**
	c.	Name the three main prerequisites for digital evidence to be admissible in court.	**5 Marks**	**L1**	**CO1**

13.	**a.**	Compare and contrast the structure and forensic artifacts of the FAT32 and NTFS file systems.	**10 Marks**	**L2**	**CO2**
	b.	Convert the following ASCII code to text: *48 65 6C 6C 6F*.	**5 Marks**	**L2**	**CO2**
	c.	Illustrate how file carving works to recover a deleted JPEG file from unallocated space.	**5 Marks**	**L2**	**CO2**
Or					
14.	**a.**	Explain the challenges a forensic investigator faces when dealing with Solid State Drives (SSDs) compared to traditional Hard Disk Drives (HDDs).	**10 Marks**	**L2**	**CO2**
	b.	Classify the following file formats based on their headers: *%PDF, PK, FF D8 FF*.	**5 Marks**	**L2**	**CO2**
	c.	Select a suitable method to extract a forensic artifact like browser history and justify your choice.	**5 Marks**	**L2**	**CO2**

15.	**a.**	Compare the steps taken by a computer forensic specialist during a corporate espionage investigation versus a child exploitation investigation.	**10 Marks**	**L3**	**CO3**

	b.	Explain how 'Information Warfare' tools can be used for corporate surveillance.	**5 Marks**	**L3**	**CO3**
	c.	Differentiate between the roles of a hacker and an organized crime syndicate in the theft of intellectual property.	**5 Marks**	**L3**	**CO3**
		Or			
16.	**a.**	Describe the process of 'Searching and Seizing Computer-Related Evidence' while adhering to legal protocols.	**10 Marks**	**L3**	**CO3**
	b.	Summarize the future issues anticipated in the field of computer forensics due to emerging technologies.	**5 Marks**	**L3**	**CO3**
	c.	Categorize the following as a 'Surveillance Tool', 'Theft of Component', or 'Terrorism Act': (i) Keylogger, (ii) Stealing a RAM module from a server, (iii) Using encrypted messaging to plan an attack.	**5 Marks**	**L3**	**CO3**

17.	**a.**	Analyze the role of data backup in the overall data recovery strategy of an organization hit by a ransomware attack.	**10 Marks**	**L3**	**CO4**
	b.	Illustrate the process of recovering data hidden using steganography in a graphic file.	**5 Marks**	**L3**	**CO4**
	c.	Propose a method to control contamination of evidence during the data collection phase.	**5 Marks**	**L3**	**CO4**
		Or			
18.	**a.**	Discuss the various 'Collection Options' available to an investigator and the 'Obstacles' associated with each when seizing evidence from a networked enterprise environment.	**10 Marks**	**L3**	**CO4**
	b.	Apply the 'Rules of Evidence' to a scenario where an employee is suspected of data theft.	**5 Marks**	**L3**	**CO4**
	c.	Formulate a checklist for the steps involved in reconstructing a cyber-attack on a web server.	**5 Marks**	**L3**	**CO4**